

PAT-NO: JP02005141565A
DOCUMENT-IDENTIFIER: JP 2005141565 A
TITLE: ELECTRONIC SEAL SYSTEM

PUBN-DATE: June 2, 2005

INVENTOR-INFORMATION:

NAME	COUNTRY
NAKANE, TAKANARI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SHACHIHATA INC	N/A

APPL-NO: JP2003378710
APPL-DATE: November 7, 2003

INT-CL (IPC): G06F017/60 , G06F012/14

ABSTRACT:

PROBLEM TO BE SOLVED: To provide an electronic seal system that enables a user unconnected to a network to use an electronic seal as in an online condition without impairing a unified management mode of electronic seals.

SOLUTION: The electronic seal system is an improved one that stores a main seal data file 6 registering each user's seal impression image data 7 in a memory means 5 of a shared computer 1. A management system 4 is additionally provided with a checkout means for lending a copy of the user's seal data file to a terminal 2 of the user, a blocking means for disabling access to the user's seal data file in the shared computer during the lending, and a check-in means for capturing a use history into the main seal data file in the shared computer when the lent seal data file is returned. An electronic seal can be thus used in an offline environment.

COPYRIGHT: (C)2005,JPO&NCIPI

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-141565

(P2005-141565A)

(43) 公開日 平成17年6月2日(2005.6.2)

(51) Int. Cl.⁷

G06F 17/60

G06F 12/14

F I

G06F 17/60 14 O

G06F 17/60 162 C

G06F 12/14 320 E

テーマコード (参考)

5B017

審査請求 未請求 請求項の数 3 O L (全 8 頁)

(21) 出願番号 特願2003-378710 (P2003-378710)

(22) 出願日 平成15年11月7日 (2003.11.7)

(71) 出願人 390017891

シヤチハタ株式会社

愛知県名古屋市西区天塚町4丁目69番地

(74) 代理人 100078101

弁理士 綿貫 達雄

(74) 代理人 100059096

弁理士 名嶋 明郎

(74) 代理人 100085523

弁理士 山本 文夫

(72) 発明者 中根 崇成

愛知県名古屋市西区天塚町4丁目69番地

シヤチハタ株式会社内

Fターム (参考) 5B017 AA06 CA16

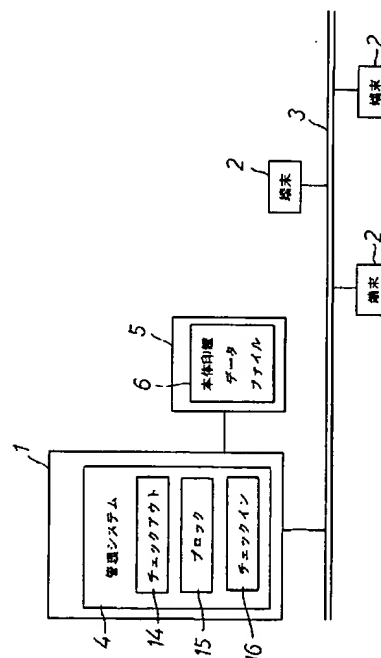
(54) 【発明の名称】 電子印鑑システム

(57) 【要約】

【課題】 電子印鑑の一元管理された管理形態を損なうことなく、ネットワークと非接続状態にあるユーザーが接続状態と同様に電子印鑑を使用できるようにした電子印鑑システムを提供する。

【解決手段】 各ユーザーの印影イメージデータ7を登録した本体印鑑データファイル6を共有コンピュータ1のメモリ手段5に記憶させた電子印鑑システムの改良である。その管理システム4に、ユーザーの端末2に対してそのユーザーの印鑑データファイルをコピーして貸し出すチェックアウト手段と、貸し出し中は共有コンピュータのそのユーザーの印鑑データファイルへのアクセスを不能にするブロック手段と、貸し出された印鑑データファイルを返却する際にその使用履歴を共有コンピュータの本体印鑑データファイルに取り込むチェックイン手段とを付加する。これにより非接続環境下における電子印鑑の使用が可能となる。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

各ユーザーの印影イメージデータをユーザー名、パスワード、使用履歴とともに登録した本体印鑑データファイルを共有コンピュータのメモリ手段に記憶させ、ユーザーは端末からネットワークを介して共有コンピュータの管理システムにログオンして上記本体印鑑データファイルから取り出した印影イメージデータを電子文書に捺印する電子印鑑システムにおいて、前記管理システムが、ユーザーの端末に対してそのユーザーの印鑑データファイルをコピーして貸し出すチェックアウト手段と、貸し出し中は共有コンピュータのそのユーザーの印鑑データファイルへのアクセスを不能にするブロック手段と、貸し出された印鑑データファイルを返却する際にその使用履歴を共有コンピュータの本体印鑑データファイルに取り込むチェックイン手段とを有することを特徴とする電子印鑑システム。

10

【請求項 2】

ユーザーの端末に貸し出されたそのユーザーの印鑑データファイルには、その端末における印影イメージデータの使用時刻及び使用回数を記録する手段が付属していることを特徴とする請求項 1 記載の電子印鑑システム。

【請求項 3】

貸し出し中の印影イメージデータの使用時刻はそのユーザーの端末が、それ以外のコンピュータなどに接続できない場合以外には共有コンピュータのシステム時間を参照することによって一意のコンピュータ上のシステム時計を時刻取得源として利用できることを特徴とする請求項 2 記載の電子印鑑システム。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子文書にユーザー（電子文書の作成者または送信者）が印影イメージデータを添付することにより、紙文書に捺印した場合と同様の効果を得ることができる電子印鑑システムの改良に関するものである。

【背景技術】

【0002】

現在では、業務上で作成される文書の多くはコンピュータを利用して作成された電子文書であるが、上司の印鑑をもらうためなどに紙に出力している場合がある。捺印者の承認・決済などの意思を証明する捺印システムは永年にわたりわが国に定着しており、文書が電子化された現在においても堅持されている。この結果、電子文書としての利点が十分に発揮されず、捺印が必要な重要書類については電子文書化が進まないなどの問題がある。

30

【0003】

そこで近年、ネットワーク上で電子文書への電子印鑑の捺印を可能とした電子印鑑システムが開発され、多くの企業や官庁において用いられている。この電子印鑑システムは単にユーザーの印影イメージデータを電子文書に貼り付けるものではなく、印影イメージデータに電子署名、認証機関から取得した電子証明書などのセキュリティ情報を埋め込み、捺印者以外の者が印影イメージデータをコピーして不正使用した場合にはその事実を容易に発見できるようになっている。

40

【0004】

また特許文献 1 に示すように、本出願人会社が提供している電子印鑑システムでは、全ユーザー（会社の場合には全社員）の印影イメージデータをユーザー名、パスワードとともに登録した印鑑データファイルを共有コンピュータ上に置いている。そしてユーザーはネットワークにより接続された自己の端末からユーザー名、パスワードを入力して電子印鑑システムにログインし、共有コンピュータから自己の印影イメージデータを取り出して端末で作成した電子文書に捺印するようになっている。

【0005】

さらに、ユーザーが上記した電子印鑑を捺印するたびに捺印時刻、捺印カウンタのシリアルナンバーが印影イメージデータに埋め込まれるとともに、これらの情報を共有コンピ

50

ユーザ上の管理システムが一元管理し、どのユーザーが何時、どの電子印鑑を捺印したか、またその捺印は何回目であるかを記録している。これらの情報は変更できないため、捺印者以外の者が印影イメージデータをコピーした場合には、捺印カウンタ番号が同一の電子印鑑が複数存在することとなって不正使用が判明する。

【0006】

上記したように、電子印鑑システムはセキュリティを保持しつつ、ネットワーク上で電子文書への電子印鑑の捺印が可能なシステムである。しかし上記の電子印鑑システムは、ネットワークを介して共有コンピュータ上の印鑑データファイルにログインするシステムであるため、出張先で自己のノートコンピュータで電子文書を作成した場合のようにネットワークとの接続ができないローカル環境下においては、電子印鑑を呼び出して使用できないという問題が生じている。

【特許文献1】特開2003-169051号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

本発明は上記した従来の問題点を解決して、電子印鑑の一元管理された管理形態を損なうことなく、ネットワークと非接続状態にあるユーザーが接続状態と同様に電子印鑑を使用できるようにした電子印鑑システムを提供することを目的とするものである。

【課題を解決するための手段】

【0008】

上記の課題を解決するためになされた本発明の電子印鑑システムは、各ユーザーの印影イメージデータをユーザー名、パスワード、使用履歴とともに登録した本体印鑑データファイルを共有コンピュータのメモリ手段に記憶させ、ユーザーは端末からネットワークを介して共有コンピュータの管理システムにログオンして上記本体印鑑データファイルから取り出した印影イメージデータを電子文書に捺印する電子印鑑システムにおいて、前記管理システムが、ユーザーの端末に対してそのユーザーの印鑑データファイルをコピーして貸し出すチェックアウト手段と、貸し出し中は共有コンピュータのそのユーザーの印鑑データファイルへのアクセスを不能にするブロック手段と、貸し出された印鑑データファイルを返却する際にその使用履歴を共有コンピュータの本体印鑑データファイルに取り込むチェックイン手段とを有することを特徴とするものである。

【0009】

なお、ユーザーの端末に貸し出されたそのユーザーの印鑑データファイルには、その端末における印影イメージデータの使用時刻及び使用回数を記録する手段を付属させておくことが好ましい。また、貸し出し中の印影イメージデータの使用時刻はそのユーザーの端末がそれ以外のコンピュータなどに接続できない場合以外に共有コンピュータのシステム時間を参照することによって一意のコンピュータ上のシステム時間を時刻取得源としていることが好ましい。

【発明の効果】

【0010】

本発明の電子印鑑システムは、ユーザーが端末からネットワークを介して共有コンピュータの管理システムにログオンできる通常的环境下においては、従来と同様に共有コンピュータの本体印鑑データファイルから取り出した印影イメージデータを電子文書に捺印することができる。この环境下においては、全ての電子印鑑の捺印時刻、捺印カウンタのシリアルナンバーなどの情報を共有コンピュータ上の管理システムが一元管理している。

【0011】

また出張先などにおいて自己の電子印鑑を使用したいユーザーは、予め共有コンピュータにログオンしてその管理システムのチェックアウト手段を用い、そのユーザーの印鑑データファイルをユーザーの端末に対して貸し出しを受けておく。このチェックアウトの手続により、ユーザーは自己の端末において電子印鑑の捺印が可能となる。なおユーザーの端末に貸し出された印鑑データファイルには、その端末における印影イメージデータの使

用時刻及び使用回数を記録する手段を付属させておく。この貸し出し期間中は、共有コンピュータのそのユーザーの印鑑データファイルへのアクセスを不能にしておき、他人による使用を防止する。

【0012】

出張から戻ったユーザーは、自己の端末から共有コンピュータにログオンしてその管理システムのチェックイン手段を用い、貸し出された印鑑データファイルを返却するが、その際に自己の端末に記憶されている電子印鑑の使用履歴が、共有コンピュータの本体印鑑データファイルに書き込まれる。このため共有コンピュータの管理システムによる電子印鑑の一元管理された管理形態が損なわれることがない。このようにして本発明によれば、ネットワークと非接続状態にあるユーザーが接続状態と同様に電子印鑑を使用できるようになる。

10

【発明を実施するための最良の形態】

【0013】

以下に図面を参照しつつ、本発明の好ましい実施形態を説明する。

図1は電子印鑑システム全体の説明図であり、共有コンピュータ1と多数のユーザーの端末2とがネットワーク3を介して接続された状態を示している。共有コンピュータ1には電子印鑑システムの管理システム4がセットされている。また共有コンピュータ1のメモリ手段5には、管理システム4によって制御される本体印鑑データファイル6が記憶されている。

【0014】

この本体印鑑データファイル6には、図2に示すように各ユーザーの印影イメージデータ7、ユーザー名8、パスワード9、使用履歴10などが全ユーザーにつき登録されている。使用履歴10は、印影イメージデータ7毎の捺印時刻11、捺印カウンタのシリアルナンバー12その他の情報を含むものである。このほか、認証機関から取得した電子証明書などのセキュリティ情報13を含ませることができる。

20

【0015】

通常的环境下においては、ユーザーは自己の端末2からユーザー名、パスワードを入力してネットワーク3を介して共有コンピュータ1の管理システム4にログオンし、本体印鑑データファイル6から自己の印影イメージデータ7を読み出して端末2上で作成した電子文書に電子印鑑を捺印することができる。なお前記したように、管理システム4は全ての印影イメージデータ7につきその捺印時刻と捺印回数を一元管理している。

30

【0016】

以上に説明した内容は従来の電子印鑑システムと同じであるが、本発明では図1に示すように、共有コンピュータ1の管理システム4に、チェックアウト手段プログラム14と、ブロック手段プログラム15と、チェックイン手段プログラム16とを組み込んである。

【0017】

チェックアウト手段プログラム14は、ユーザーの端末2に対してそのユーザーの印鑑データファイルをコピーして貸し出すチェックアウト機能を備えたものである。すなわち図3に示すように、ネットワーク3から切り離された環境下で自己の電子印鑑を使用したユーザーは、予めネットワーク3を介して共有コンピュータ1の管理システム4にログインし、チェックアウト手段プログラム14に対してユーザーの印鑑データファイルの貸し出しを要求する。チェックアウト手段プログラム14はメモリ手段5に記憶された本体印鑑データファイル6から要求された印鑑データファイルを、ユーザーの端末2にコピーして貸し出す。

40

【0018】

この貸し出しは単なる印鑑データファイルのコピーであるが、現物の印鑑を貸し出した場合と同様の状況とするために、チェックアウト手段による貸し出しと同時にブロック手段プログラム15が働き、貸し出し期間中は共有コンピュータ1のそのユーザーの印鑑データファイルへのアクセスを不能にする。これによって貸し出された電子印鑑については

50

他人はもちろん、本人であっても使用不能の状態となり、不正使用が防止される。この状態は下記のチェックインによって解除することができる。

【0019】

印鑑データファイルの貸し出しを受けたユーザーは、ネットワーク3と非接続の状況下においても、接続状態と同様に自己の電子印鑑を使用し、電子文書への捺印ができることとなる。このため出張先などにおいても電子印鑑システムを利用できる。このユーザーの端末2に貸し出されたそのユーザーの印鑑データファイルには、その端末2における印影イメージデータの使用時刻及び使用回数を記録する手段が付属している。ただし使用時刻はそのユーザーの端末2のシステム時計から取得して記録する。

【0020】

出張などから戻ったユーザーは、ネットワーク3を介して共有コンピュータ1の管理システム4にログインし、チェックイン手段プログラム16を用いて貸し出された印鑑データファイルを返却するチェックインを行う。このとき、チェックイン手段プログラム16はユーザーの端末のメモリ手段からその使用履歴を読み出し、共有コンピュータ1の本体印鑑データファイル6に取り込む。

【0021】

このとき同時に本体印鑑データファイル6内のデータにチェックアウト手段を行なうからチェックイン手段を行なうまでに使用した記録情報を同期させて書き込む。これによって貸し出し期間中における電子印鑑の使用状況も共有コンピュータ1の管理システム4による一元管理に組み込まれ、一元管理形態が損なわれることもない。なお、チェックインと同時にブロック手段プログラム15は停止し、通常の管理状態に戻ることもなる。

【0022】

なお、図4は本発明で用いられる共有コンピュータ1におけるハードウェア資源の利用状態を示すブロック図である。また図5はログイン処理のプロセスを示すフロー図、図6はチェックアウト手段を示すフロー図、図7はチェックイン手段を示すフロー図である。

【0023】

以上の説明では、各ユーザーが単一の印影イメージデータ7を持つものとして説明したが、特許文献1に示されたように同一ユーザーが複数種類の印影イメージデータ7を使い分けることも可能である。また印影イメージデータ7に埋め込まれている各種のセキュリティ情報も同時に貸し出されるため、端末2に貸し出しを受けたユーザーは、電子署名等と組み合わせた電子印鑑の使用も可能となる。このようにして、本発明によれば電子印鑑の一元管理された管理形態を損なうことなく、ネットワークと非接続状態にあるユーザーが接続状態と同様に電子印鑑を使用することができる。

【0024】

また本発明によれば、経理部門などの使用頻度の高い電子印鑑をシステムから切り離して1日使用し、1日分の使用履歴をまとめて共有コンピュータ1の管理システム4に読み込ませるといった使い方も可能となる。特にユーザー数が1000を越える場合には各ユーザーからの共有コンピュータ1へのアクセスが集中する時間帯にはシステムの応答速度が低下する可能性があるが、本発明により使用頻度の高い電子印鑑をシステムから切り離し、夜間などに共有コンピュータ1の管理システム4にチェックインすることとすれば、システムの負担を軽減できる効果もある。

【図面の簡単な説明】

【0025】

【図1】本発明の電子印鑑システム全体の説明図である。

【図2】本体印鑑データファイルの構成説明図である。

【図3】本発明の電子印鑑システムの使用状態の説明図である。

【図4】共有コンピュータにおけるハードウェア資源の利用状態を示すブロック図である。

【図5】ログイン処理のプロセスを示すフロー図である。

【図6】チェックアウトのプロセスを示すフロー図である。

【図 7】チェックインのプロセスを示すフロー図である。

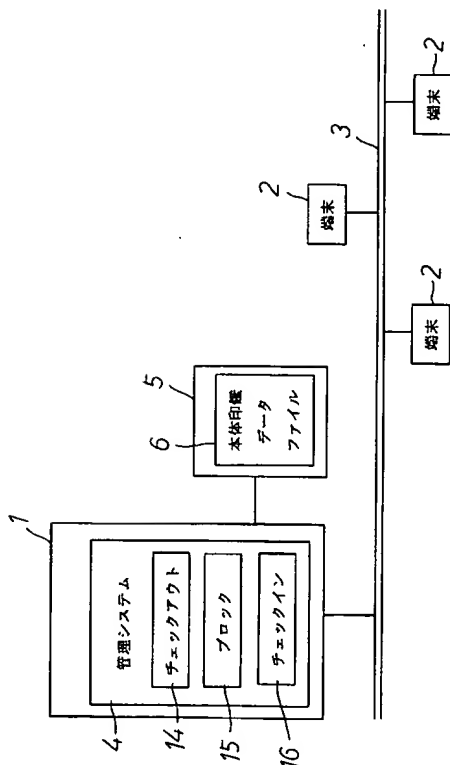
【符号の説明】

【0026】

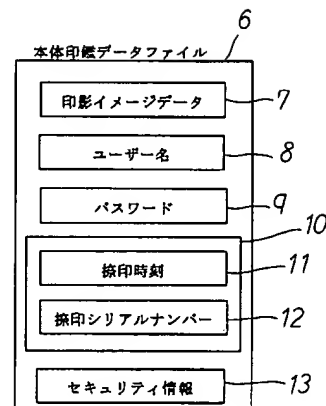
- 1 共有コンピュータ
- 2 ユーザーの端末
- 3 ネットワーク
- 4 管理システム
- 5 共有コンピュータのメモリ手段
- 6 本体印鑑データファイル
- 7 印影イメージデータ
- 8 ユーザー名
- 9 パスワード
- 10 使用履歴
- 11 捺印時刻
- 12 捺印カウンタのシリアルナンバー
- 13 セキュリティ情報
- 14 チェックアウト手段プログラム
- 15 ブロック手段プログラム
- 16 チェックイン手段プログラム

10

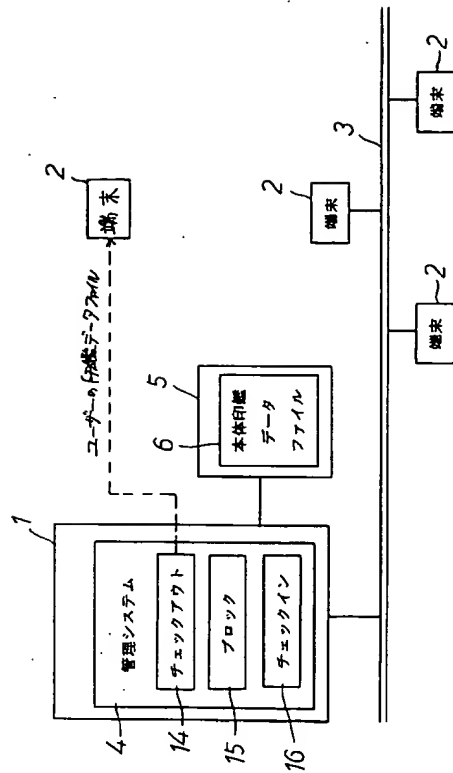
【図 1】



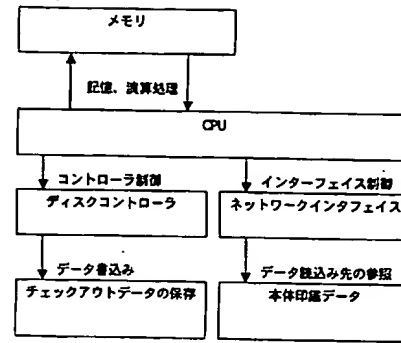
【図 2】



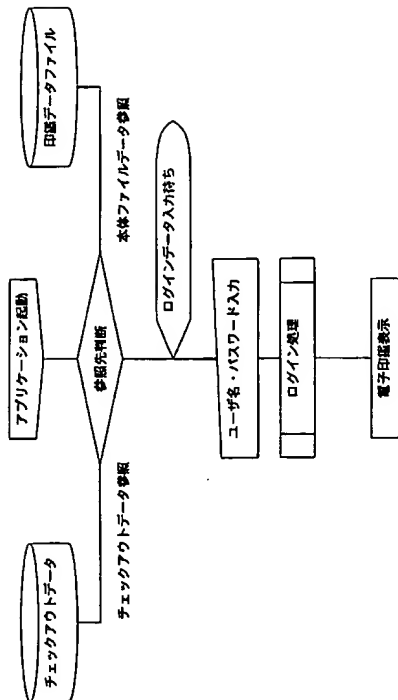
【図3】



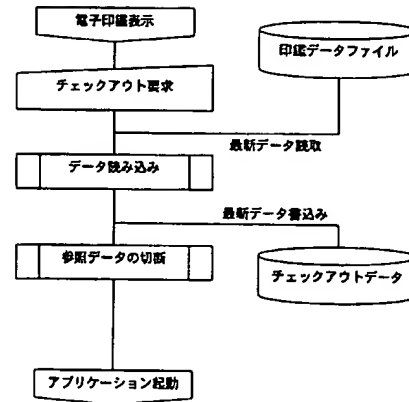
【図4】



【図5】



【図6】



【図 7】

